

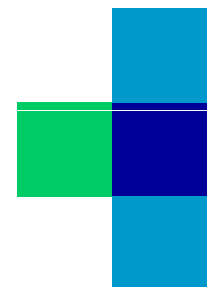
Datenschutz und Datensicherheit und ihre Anforderungen an den Betrieb von IT-Systemen, insb. KIS, RIS, PACS

DICOM 2008

KIS – RIS - PACS und 10. DICOM Treffen, Mainz, 4. – 5. Juli 2008

Dr. Manfred Brunner

**Universitätsklinikum
Erlangen**



04.07.2008

Worum geht es?

■ Ärztliche Schweigepflicht

„Was immer ich sehe und höre bei der Behandlung oder außerhalb der Behandlung im Leben der Menschen, so werde ich von dem, was niemals nach draußen ausgeplaudert werden soll, schweigen, indem ich alles Derartige als solches betrachte, das nicht ausgesprochen werden darf“

Folgerungen:

- Anvertrautes darf nicht unbefugt offenbart werden
- Das Arztgeheimnis gilt auch gegenüber nicht behandelnden Ärzten

➤ **Die ärztliche Schweigepflicht ist eine auf den Arzt bezogene Pflicht**



... und worum geht es noch?

■ Grundgesetz

- Die Würde des Menschen ist unantastbar.
- Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit.

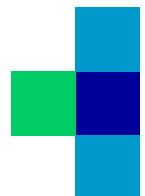
■ Recht auf informationelle Selbstbestimmung

- Jeder Einzelne darf grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen. Er muss selbst entscheiden können, wer was über ihn weiß und zu welchen Zwecken er dieses Wissen verwendet.
- Im Krankenhaus soll Datenschutz den Patienten davor schützen, dass Informationen über seinen Gesundheitszustand ohne Rechtsgrundlage erhoben, verarbeitet oder weitergegeben werden.

■ Neues Grundrecht

- Das allgemeine Persönlichkeitsrecht umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. (BVG, Urteil vom 27. 2. 2008)

➤ **Datenschutz ist ein Grundrecht des Patienten**



Harte Strafen!

■ Strafgesetzbuch

1. Wer unbefugt ein zum persönlichen Lebensbereich gehörendes Geheimnis offenbart, das ihm als
 1. Arzt ... oder Angehörigen eines andere Heilberufs anvertraut worden oder sonst bekannt geworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.
3. Den im Absatz 1 Genannten stehen ihre berufsmäßig tätigen Gehilfen gleich
4. ... auch anzuwenden nach dem Tod des Betroffenen
5. Handelt der Täter gegen Entgelt, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

■ Datenschutzgesetze

- Schadensersatz
- Bußgeld (bis 250 T€)



Was kann denn schon passieren?

- Welche Formen von Missbrauch wären möglich, wenn Patientendaten in die Hände unberechtigter Dritter gelangten?
 - Für den Patienten?
 - Für das Krankenhaus?
- Welche Folgen hätte es, wenn Patientendaten verändert würden?
 - Lebensgefahr?
- Was würde geschehen, wenn im Klinikumsnetzwerk plötzlich wichtige Computer oder andere IT-Komponenten für einen längeren Zeitraum ausfielen?
 - Wie hoch wäre der Schaden?
 - Wann und wie könnte die Arbeit fortgesetzt werden?



Populäre (gewagte) Behauptungen

- Wir haben doch nichts zu verbergen!
- Das gerät doch bald in Vergessenheit!
- Gesundheitsdaten interessieren doch niemand!
- Unsere Daten sind sicher!
- Bei uns ist noch nie etwas passiert!
- Es hat keinen Sinn, Regelungen zu erlassen, weil sich sowieso keiner daran hält!
- Es regelt sich alles von selbst!
- Ein Arzt macht so etwas nicht!



Arzt – Patientenverhältnis

Arzt – Patient



- + Krankenkasse
- + Geräte
- + Wissende Geräte
- + Vernetzung
- + Wissen
- + Fremde
- + Verteiltes Wissen

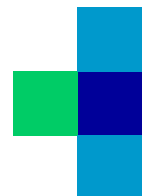
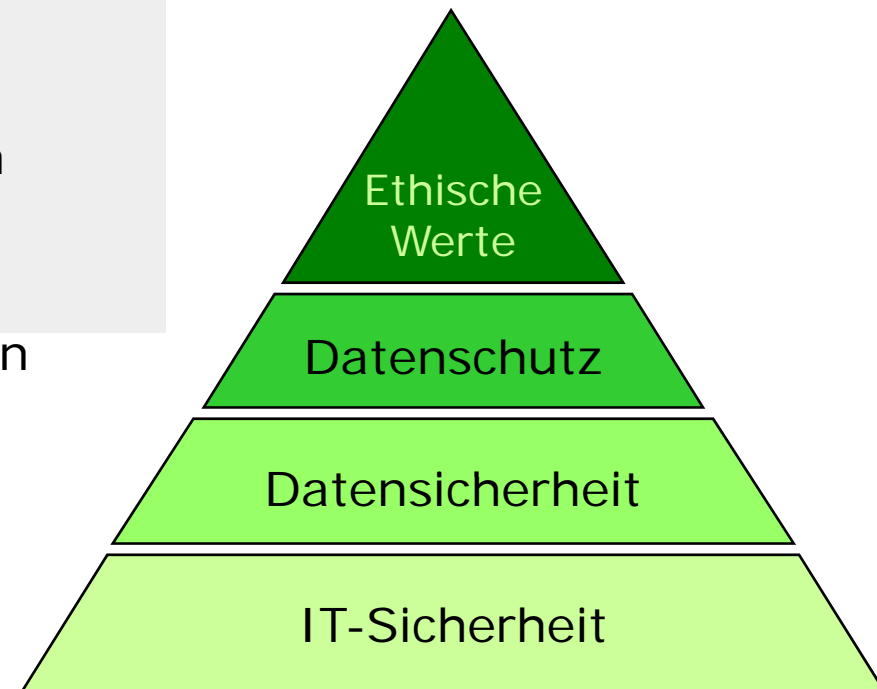
Grundlagen

Vertrauen

Misstrauen

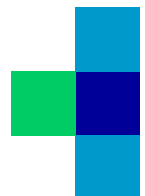
Abhilfe

Datenschutz-Pyramide



Was ist an Patientendaten besonders?

- Der Patient muss sich darauf verlassen können, dass die Daten zu seiner Person und die Informationen, die er über sich preisgibt, nicht ohne seinen Willen und ohne sein Wissen weiterverwendet werden.
- Angaben über Gesundheit oder Sexualleben sind besonders sensitiv
 - sind unter Umständen von lebenserhaltender Bedeutung
 - enthalten intime Details über Körper, Psyche, Sexualität, genetische Disposition
- Dokumentationspflicht
 - Feststellungen und Maßnahmen im Rahmen von Anamnese, Diagnose und Therapie müssen ordnungsgemäß dokumentiert und sachgerecht für mindestens 10 Jahre aufbewahrt werden.
- Zweck
 - Verwendung durch behandelnde Ärzte für Dokumentation, Therapie, Abrechnung
 - Verwendung durch Patienten zur Information und Kontrolle
 - Verwendung durch Dritte zur Beweis- und Qualitätssicherung, Kostenträgerkontrolle



Datenschutzrechtliche Anforderungen

- Vertraulichkeit
Nur Befugte dürfen patientenbezogene Daten zur Kenntnis nehmen.
- Authentizität
Der Urheber bzw. der Verantwortliche muss eindeutig feststellbar sein.
- Integrität
Patientendaten müssen unversehrt, vollständig und gültig sein.
- Verfügbarkeit
Daten müssen zeitgerecht zur Verfügung stehen.
- Revisionsfähigkeit
Die Verarbeitungsprozesse müssen nachvollzogen werden können.
- Validität
Die Verarbeitungsqualität muss für den Nutzungszweck angemessen sein.
- Rechtssicherheit
Nachweise der Verarbeitung müssen Beweiskraft haben.
- Nutzungsfestlegung
Zugriffe werden über ein Berechtigungskonzept geregelt
- Transparenz
Information über Verarbeitung und Nutzung der Daten.



Maßnahmen

- **Verschlüsselung**
 - Vertraulichkeit
 - bei zentralen Systemen: auf Transport/Leitungsebene
 - bei dezentralen Systemen: auf Anwendungsebene
- **Signatur**
 - Authentizität, Integrität, Revisionsfähigkeit
- **Qualifizierte Signatur**
 - Rechtssicherheit
- **Systemarchitektur**
 - Verfügbarkeit, Validität
- **Protokollierung**
 - Revisionsfähigkeit
- **Auskunftsfunction**
 - Transparenz
- **Pseudonymisierung**
 - löst den Personenbezug auf



Nutzungsfestlegung

■ Grundsätze:

- Kein Zugriff aller Abteilungen auf alle Patientendaten
- Zugriffsrechte für die behandelnde Fachabteilung
- Abteilungsübergreifende Zugriffe bei Behandlungszusammenhang nach Erforderlichkeit
- Sonderfall: Notfallkennung (Protokollierung)
- Detaillierte Rechte (Lesen, Schreiben, Ändern, Ausführen)

■ Berechtigungskonzepte

- Musketierkonzept (Einer für Alle , Alle für Einen!)
- Rollenkonzept
 - Zugriffsmatrix
- Anforderungskonzept
 - Nur der behandelnde Arzt hat die Zugriffsberechtigung und reicht sie bei Anforderung einer Leistung weiter



Fazit

■ entweder

- technologische Entwicklungen nutzen
 - Verschlüsselung, Signatur
- Berechtigungskonzepte erarbeiten und umsetzen

■ oder

- zurück zur Papierakte
- dem Patienten die Bilder in die Hand drücken
- Augen zu und durch und abwarten, was passiert

